U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Incident Management Analysis and Reporting System (IMARS)
Bureau/Office: Office of the Secretary
Date: September 30, 2017
Point of Contact:
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Incident Management Analysis and Reporting System (IMARS) is an enterprise-wide incident management and reporting commercial-off-the-shelf (COTS) product managed by the Department of the Interior (DOI) Office of Law Enforcement and Security (OLES). IMARS tracks law enforcement incidents and allows sharing of incident or suspicious activity information with Federal agencies and

other law enforcement organizations. This information will be used to collaborate with these organizations on law enforcement activities.
IMARS will enhance the following abilities:

- Prevent, detect and investigate known and suspected criminal activity.
- Protect natural and cultural resources.
- Capture, integrate and share law enforcement and related information and observations from other sources.
- Identify needs (training, resources, etc.).
- Measure performance of law enforcement programs and management of emergency incidents.
- Meet reporting requirements including DOI Level 1 and Level 2 Significant Incidents, and Department of Homeland Security and National Incident Based Reporting System.
- Analyze and prioritize protection efforts.
- Justify requests and expenditures.
- Assist in managing visitor use and protection programs.
- Training (including, incorporating into Federal Law Enforcement Training Center programs)
- Investigate, detain and apprehend those committing crimes on DOI lands.
- Investigate and prevent visitor accident injuries on DOI lands.

C. What is the legal authority?

Uniform Federal Crime Reporting Act, 28 U.S.C. § 534; Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108-458); Homeland Security Act of 2002 (Pub. L. 107-296); USA PATRIOT ACT of 2001 (Pub. L. 107-56); USA PATRIOT Improvement Act of 2005 (Pub. L. 109-177); Tribal Law and Order Act of 2010 (Pub. L. 111-211); Homeland Security Presidential Directive 7 - Critical Infrastructure Identification, Prioritization, and Protection; Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors; and Criminal Intelligence Systems Operating Policies, 28 CFR Part 23.

D. Why is this PIA being completed or modified?

☐New Information System
☐New Electronic Collection
☒Existing Information System under Periodic Review
☐Merging of Systems
☐Significantly Modified Information System
☐Conversion from Paper to Electronic Records
☐Retiring or Decommissioning a System
☐Other: *Describe*

E. Is this information system registered in CSAM?

☒Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-00-01-05-01-0018-00; Incident Management Analysis and Reporting System (IMARS) System Security Plan

☐No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒Yes: *List Privacy Act SORN Identifier(s)*

DOI-10, Incident Management, Analysis and Reporting System (IMARS), 79 FR 31974, June 3, 2014. The DOI-10, IMARS SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108.

☐No

H. Does this information system or electronic collection require an OMB Control Number?

☐Yes: *Describe*
☒No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒Name
☒Citizenship
☒Gender
☒Birth Date
☒Group Affiliation
☒Marital Status
☒Biometrics
☒Other Names Used
☒Truncated SSN
☒Legal Status
☒Place of Birth
☒Religious Preference
☒Security Clearance
☒Spouse Information
☒Financial Information
☒Medical Information
☒Disability Information
☒Credit Card Number
☒Law Enforcement
☒Education Information
☒Emergency Contact
☒Driver's License
☒Social Security Number (SSN)
☒Personal Cell Telephone Number
☒Tribal or Other ID Number
☒Personal Email Address
☒Mother's Maiden Name
☒Home Telephone Number
☒Child or Dependent Information
☒Employment Information
☒Military Status/Service
☒Mailing/Home Address
☒Race/Ethnicity

☒Other: *Specify the PII collected.*

IMARS contains law enforcement incident reports, law enforcement personnel records, and law enforcement training records, which contain the following information: Social Security numbers (SSNs), driver's license numbers, vehicle identification numbers, license plate numbers, names, home addresses, work addresses, telephone numbers, email addresses and other contact information, emergency contact information, ethnicity and race, tribal identification numbers or other tribal enrollment data, work history, educational history, affiliations, and other related data, dates of birth, places of birth, passport numbers, gender, fingerprints, hair and eye color, and any other physical or distinguishing attributes of an individual. The system contains images and videos collected from audio/visual recording devices such as surveillance cameras, closed circuit television located at DOI facilities for security and/or law enforcement operations, a mobile video recorder installed on a patrol vehicle and a wearable video recorder (i.e., body-worn cameras) for authorized law enforcement operations. The privacy implications of wearable video recordings are addressed separately in the Digital Evidence Management System privacy impact assessment currently under development.

Incident reports and records may include attachments such as photos, video, sketches, medical reports, and email and text messages, and information concerning criminal activity, response, and outcome of the incident. Reports and records may include information related to incidents occurring on Tribal reservations at the Bureau of Indian Affairs or tribal schools. School incident information may include injuries that are physical, emotional or sexual in nature, including but are not limited to the following: date of birth, age, suspected abuse (Physical, Emotional, Sexual), alleged offender name, potential witness name, etc. Records in this system also include information concerning Federal civilian employees and contractors, Federal, tribal, state and local law enforcement officers and may contain information regarding an officer's name, contact information, station and career history, firearms qualifications, medical history, background investigation and status, date of birth and SSN. IMARS also contains information regarding officers' equipment, such as firearms, tasers, body armor, vehicles, computers and special equipment-related skills.

B. What is the source for the PII collected? Indicate all that apply.

☒Individual
☒Federal agency
☒Tribal agency
☒Local agency
☒DOI records
☒Third party source
☒State agency
☐Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☒Paper Format
☒Email
☒Face-to-Face Contact

☒Web site
☒Fax
☒Telephone Interview
☒Information Shared Between Systems
☒Other: *Describe*

Data may be collected from telephone, text message or email records obtained from cellular carriers, internet service providers, and other companies. Information may also be obtained from public access web sites, newspapers, press releases, or other sources. Information may also be obtained through data feeds to other Law Enforcement databases or systems. Information may be derived from other Federal systems to share information across the Law Enforcement community. Data feeds will be established using the IMARS application programming interface (API). The API sets a standard process of how third party applications would submit or retrieve data from IMARS. It runs on top of the standard secure web protocol (HTTPS) ensuring data is encrypted from end to end. Between applications, data is exchanged in common web format. The user's credentials are submitted to the API to perform a certain action and based on his/her role it will be executed in the IMARS report system. The results of the action submitted can then be displayed in the third party application for immediate feedback.

D. What is the intended use of the PII collected?

Data collected in the IMARS system is used to record information related to an incident investigation on land/areas governed by the DOI as well as tribal lands. Data is held in a database repository or facilities controlled and maintained by authorized personnel.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

PII is shared within OLES for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties.

☒Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

PII is shared with DOI bureaus and offices for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI and Tribal properties.

☒Other Federal Agencies: *Describe the federal agency and how the data will be used.*

PII is shared with other Law Enforcement agencies for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties. Information may also shared between DOI Law Enforcement and other Federal agencies. Information may also be shared with other Federal agencies as authorized and described in the routine uses published in the DOI-10 IMARS system of records notice, which may be viewed at: https://www.doi.gov/privacy/sorn.

☒Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

PII is shared with Tribes for investigation, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties which might include Tribal lands.

☒Contractor: *Describe the contractor and how the data will be used.*

PII is shared with DOI contractors who facilitate background investigations for hiring purposes, and to facilitate system operation.

☒Other Third Party Sources: *Describe the third party source and how the data will be used.*

PII is shared with attorneys or court staff for judicial reasons. Information may also be shared with other third parties as authorized and described in the routine uses published in the DOI-10 IMARS system of records notice, which may be viewed at: https://www.doi.gov/privacy/sorn.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

In some cases individual members of the public may decline to provide information where providing information is voluntary, and are informed of this right by the officer. Due to the purpose and nature of the system, to support law enforcement investigation, there may be many cases where individuals will not have the opportunity to consent to the collection or use of their information. For use of audio and visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some DOI controlled areas may have signs posted that inform individuals of surveillance activities, but in many cases notice may not be provided or consent obtained for audio or images captured during law enforcement activities.

☐No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐Privacy Act Statement: *Describe each applicable format.*

☒Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this privacy impact assessment and the DOI-10, IMARS system of records notice, which may be viewed on the DOI SORN website at https://www.doi.gov/privacy/doi-notices.

☐Other: *Describe each applicable format.*

☒None

In some cases, such as for use of audio and visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some DOI controlled areas may have signs posted that inform individuals of surveillance activities, but in many cases notice may not be provided or consent obtained for audio or images captured during law enforcement activities.

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data is retrieved by name, SSN, home address, work address, phone numbers, emergency contact information, driver's license or other forms of ID, ethnicity and race, date of birth, gender, physical description of the individual including any and all physical attributes, and incident data.

I. Will reports be produced on individuals?

☒Yes: *What will be the use of these reports? Who will have access to them?*

Authorized IMARS users can manually run reports for investigative purposes. The following reports are available to authorized users: Be On The Lookout (BOLO), Request for Identification Report, Criminal History Report, and Missing Person (also called Amber/Silver) report. A user is authorized based on the group role or roles assigned to the individual user. In addition, incident, supplemental, crash, arrest, ticket, and suspicious activity reports can be produced. Detailed information can be viewed by authorized users including incident, person, property, vehicle, address, etc. Administrative reports may also be generated in response to audits, oversight, and compliance.

☐No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

The system provides basic accuracy checking. The individual collecting the data will verify the accuracy of data collected per policy and procedures defined by each participating organization. Supervisors will also review data for accuracy.

B. How will data be checked for completeness?

The system provides basic completeness checking. The individual collecting the data will verify the completeness of data collected per policy and procedures defined by each participating organization. Supervisors will also review data for completeness.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Individual IMARS users, including supervisors, are responsible for ensuring the data is current. Law Enforcement Officers ensure information is current through validation with applicable law enforcement systems.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

IMARS records are retained and disposed of in accordance with Office of the Secretary Records Schedule, Item 8151, Incident, Management, Analysis and Reporting, which was approved by the National Archives and Records Administration (NARA) (N1-048-09-05), and other NARA approved bureau or office records schedules. Incident data will be cut-off when an incident is closed off. The data will be archived 20 years after cut-off and destroyed 50 years after archiving. Non-incident data includes data relating to the user/officer and their unit of assignment, badge number, training, qualifications, etc. This data will be cut-off after the user/officer retires, resigns, leaves the DOI, or is assigned to a position that no longer requires access to IMARS. This data is archived three years after cut-off and destroyed 50 years after archiving.

Video records are managed in accordance with DAA-0048-2015-0002-0001, Routine Surveillance Recordings, which provides that recordings of a non-evidentiary value will be destroyed after 30 days. Videos associated with criminal incidents in the database will be maintained as evidence according to the incident's disposition schedule.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA guidelines and 384 Departmental Manual 1. Archival and disposition of records will be accomplished within the automated records retention functions built in the system and procedures will follow applicable guidance by NARA, applicable legislation such as the Federal Records Act, and Departmental guidance. The procedures are documented in the IMARS Records Management Plan and approved by NARA.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a risk to the privacy of individuals in IMARS due to the amount of sensitive PII maintained for law enforcement incident reports, law enforcement investigations, and law enforcement personnel and training records. The risks are mitigated by controls implemented to limit unauthorized exposure of PII. Only authorized personnel with proper credentials can access the records in the system. DOI requires two-factor authentication for network and system access; system access is based on least privilege

access and role-based access controls; access control lists were created and segmented by bureau; users cannot view information for other users unless specifically authorized.

Privacy risks exist with authorized data sharing with other law enforcement organizations. Risks may include but are not limited to data integrity, loss of data and data confidentiality for data shared and controlled by other organizations. A MOU will be established with agencies and organizations to ensure adequate controls are in place to protect privacy. Some examples of these controls include those listed above as well as the following:

- MOUs established between agencies defining system access rules and policies
- Limiting information at the source (IMARS connection) deployed to outside agencies
- Utilizing Secure File Transfer Protocols for transmission of information
- Security of systems receiving information shared
- Access restrictions to authorized officials
- Authorized use of information shared
- Limits on uses and additional sharing
- Retention periods and authorized destruction or return of information shared

There is also a privacy risk for the use of audio/visual recording devices, such as body cameras, dashboard cameras, and hand-held cameras, used for routine law enforcement purposes, to enhance officer safety, promote cost savings, assist in crime prevention, and support law enforcement investigations. These cameras may be worn by DOI bureau and office law enforcement officials, placed on the dashboard of law enforcement vehicles, or used by individual law enforcement officials on properties and locations within the jurisdiction of the DOI, including Federal facilities, national monuments, national parks, tribal lands, and public lands to include buildings, housing units, roadways, trails, and bridges/tunnels, and law enforcement offices and jail units; National Wildlife Refuges; national dams and hydroelectric power plants.

These devices may capture audio and images of persons, places and events occurring in real time as part of ongoing law enforcement operations, such as identifying persons involved in potential criminal activity, or persons or vehicles fleeing from law enforcement officials. Some devices may capture metadata about the audio, images or recordings, such as time, location and date the audio, images or video were captured. Users may use settings to zoom in for persons or objects of specific interest, or pan areas of interest. Images or recordings could be used in any appropriate law enforcement investigation related to a potential criminal activity, including identification of suspects and providing evidence that may be used in proceedings.

Some privacy concerns are that devices may collect more information that is necessary to accomplish law enforcement purposes. The devices are used only by authorized law enforcement officials and only to support law enforcement activities and investigations, prevent crime, and enhance officer safety. Only the images or video feed needed to respond to unlawful activities or support investigations and prosecutions will be retained for use, all other video feed not required for retention will be automatically overwritten or disposed of per DOI policy.

Another concern is that the use of the audio/visual recording devices may restrict First Amendment protected activities like freedom of speech or association. The recordings are used to detect and deter criminal activity and enhance officer and citizen safety, and are not used for the sole purpose of restricting or investigating lawful activities conducted by members of the public. First Amendment activities will not be filmed for the sole purpose of identifying and recording the presence of individual participants engaged in lawful conduct. First Amendment activities may be recorded, however, for purposes of (1) documenting violations of law or civil wrongs; (2) aiding future coordination and deployment of law enforcement units; or (3) training; or (4) to mitigate or relieve overcrowding to enhance public safety.

IMARS is rated as a FISMA high system based upon the type and sensitivity of data, and requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive data contained in the system. The privacy controls are utilized to protect individual privacy, including limiting access to images or video feed that identify individuals or to specific events or investigations that are linked to individuals, to authorized users and law enforcement officials, and establishing controls on the retention of images and video feeds to the approved period necessary for law enforcement purposes in accordance with approved records retention schedules. DOI restricts the maintenance of images or video feeds not necessary for retention to the minimum necessary (30 days) in accordance with approved records retention schedules for routine surveillance motion picture and video recordings, ensures proper disposal at the end of the retention period, and establishes specific use policy and rules of behavior for the use of these audio/visual recording devices.

DOI employees and contractors must take privacy, security and records management training prior to being granted access to DOI information and information systems, and annually thereafter. Personnel with significant privacy responsibilities, such as law enforcement personnel, must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. Failure to protect PII or mishandling or misuse of PII may result in criminal, civil, and administrative penalties.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒Yes: *Explanation*

The use of IMARS is relevant and necessary to define, manage, and report on known or suspected incidents and support DOI law enforcement activities.

☐No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☒Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

IMARS supports law enforcement investigations that may involve data that identifies individuals and their related information or associations, which may be obtained from multiple sources instead of directly from the individual. There is a risk that data from different sources may be aggregated and may provide more information about an individual, and that such data may be outdated or inaccurate.

☐No

C. Will the new data be placed in the individual's record?

☒Yes: *Explanation*

New data may be included in the individual's record as necessary and required for law enforcement investigations.

☐No

D. Can the system make determinations about individuals that would not be possible without the new data?

☒Yes: *Explanation*

The purpose of IMARS is to support law enforcement activities, which may include investigations or reports that result in determinations about individuals. Reports or results of investigations may be shared internally and externally as authorized and necessary to meet criminal, civil and administrative law enforcement requirements, as outlined above in Section 2, question E, and the routine uses in the published DOI-10 IMARS system of records notice, which may be viewed at https://www.doi.gov/privacy/sorn.

☐No

E. How will the new data be verified for relevance and accuracy?

Law Enforcement Officers and their supervisors are responsible for the relevance and accuracy of the data. Data can be validated with other Federal, State and Local information databases. IMARS cannot check for accuracy of the information but it does enforce the use of correctly formatted data.

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

Below are methods used to limit exposure of PII.

- Only authorized personnel with proper credentials/background investigation can access system
- Least privilege access
- Role-based access control
- 2-factor authentication into system
- Users cannot view information for other users unless specifically authorized
- Access Control Lists were created and segmented by Bureau
- MOUs established between agencies defining system access rules and policies.
- Limiting information at the source (IMARS connection) deployed to outside agencies.
- Utilizing Secure File Transfer Protocols for transmission of information

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Requests for access for a particular user are initiated by authorized personnel at each DOI bureau or office. A Bureau Representative will evaluate the request and follow procedures to determine and grant individuals access to data. Least privileges determine that only the minimum levels of access to perform job functions are granted to users based on the users' job requirements.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Privacy Act contract clauses are included in the contract with the application developer.

☐No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐Yes. *Explanation*
☒No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒Yes. *Explanation*

The system provides the capability to identify and locate individuals. The data collected may include physical attributes of an individual (including text, photos, and video), personal and professional physical addresses, personal and professional phone numbers and email addresses as well as other individuals and associations related to the individuals.

☐No

L. What kinds of information are collected as a function of the monitoring of individuals?

The information collected may include physical locations, photos or videos of the individual and other tracking logs used in investigating a crime, such as a record of cell phone or credit card transactions.

M. What controls will be used to prevent unauthorized monitoring?

Access granted to individuals is password-protected; each person granted access to the system must be trained and individually authorized to use the system. Each user is assigned to roles which grant access to specific data within the system. IMARS also logs events including user login/logout, searches, views, printing, and data alterations which are reviewed on a regular scheduled basis. All users must complete security and privacy training and accept the DOI Rules of Behavior before accessing the system and follow established internal security protocols.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.
☒Security Guards
☒Key Guards
☒Locked File Cabinets
☒Secured Facility
☒Closed Circuit Television
☒Cipher Locks
☒Identification Badges

☒Safes
☒Combination Locks
☒Locked Offices
☐Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒Password
☒Firewall
☒Encryption
☒User Identification
☐Biometrics
☒Intrusion Detection System (IDS)
☒Virtual Private Network (VPN)
☒Public Key Infrastructure (PKI) Certificates
☒Personal Identity Verification (PIV) Card
☐Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒Periodic Security Audits
☒Backups Secured Off-site
☒Rules of Behavior
☒Role-Based Training
☒Regular Monitoring of Users' Security Practices
☒Methods to Ensure Only Authorized Personnel Have Access to PII
☒Encryption of Backups Containing Sensitive Data
☒Mandatory Security, Privacy and Records Management Training
☐Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Director, Office of Law Enforcement and Security, is the IMARS Information System Owner and the official responsible for oversight and management of the IMARS security controls and the protection of agency information processed and stored in the IMARS system. The Information System Owner and IMARS Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in the IMARS system. These officials and authorized IMARS personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendment, as well as processing complaints, in consultation with bureau and office Associate Privacy Officers.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The IMARS Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, and ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. The IMARS Information System Owner, Information System Security Officer, and authorized users are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC, DOI's incident reporting portal, and appropriate DOI officials in accordance with Federal policy and established DOI procedures.